wallarm

Application Security Platform Powered by AI

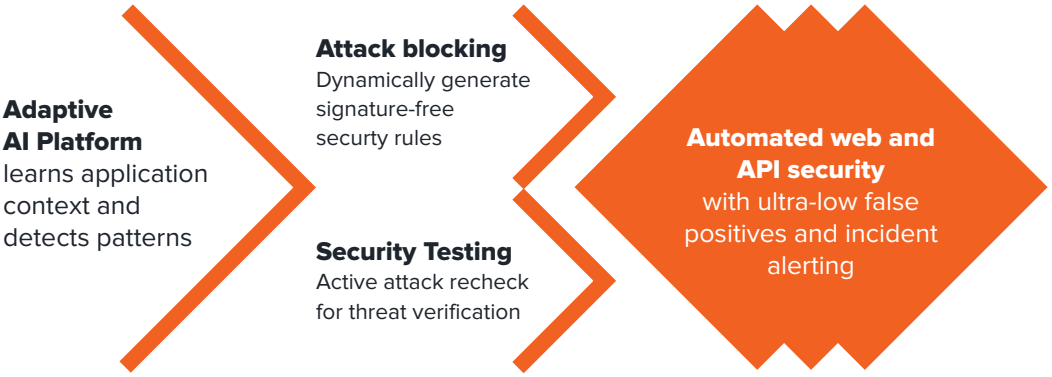
Wallarm AI-powered security platform automates application protection and security testing. Hundreds of customers already rely on Wallarm to secure websites, microservices and APIs running on private and public clouds. Wallarm AI enables application-specific dynamic WAF rules, proactively tests for vulnerabilities, and creates a feedback loop to improve detection accuracy.

wallarm.com

Adaptive application security

Key Benefits

* Adapts security rules with AI as application evolves
* Actively verifies threats to minimize manual analysis
* Protects from OWASP Top 10 and 0-day attacks
* Protects against bots and API abuse
* Lowers false-positives by customizing security rules to the application logic
* Integrates with existing infrastructure and CI/CD pipelines



Supported Platforms
Traffic filtering is performed by Wallarm nodes that can be installed on the application server, as a reverse proxy or together with the load balancer. Supported platforms include:

* As a module
  NGINX, Kong API Gateway
* As a container or VM
  Docker, VMware VM
* Linux package
  RHEL/CentOS, Debian, Ubuntu

Public Clouds Support
AWS, MS Azure, Google / GCP, Heroku

Native Support for API and HTTP Protocols
HTTP / 2.0, WEBSOCKETS, REST API, JSON, XML, SOAP

Application Stack Agnostic
NodeJS, Go, Ruby / RoR, PHP, .Net, Java, Python SAP, Oracle BS, SharePoint

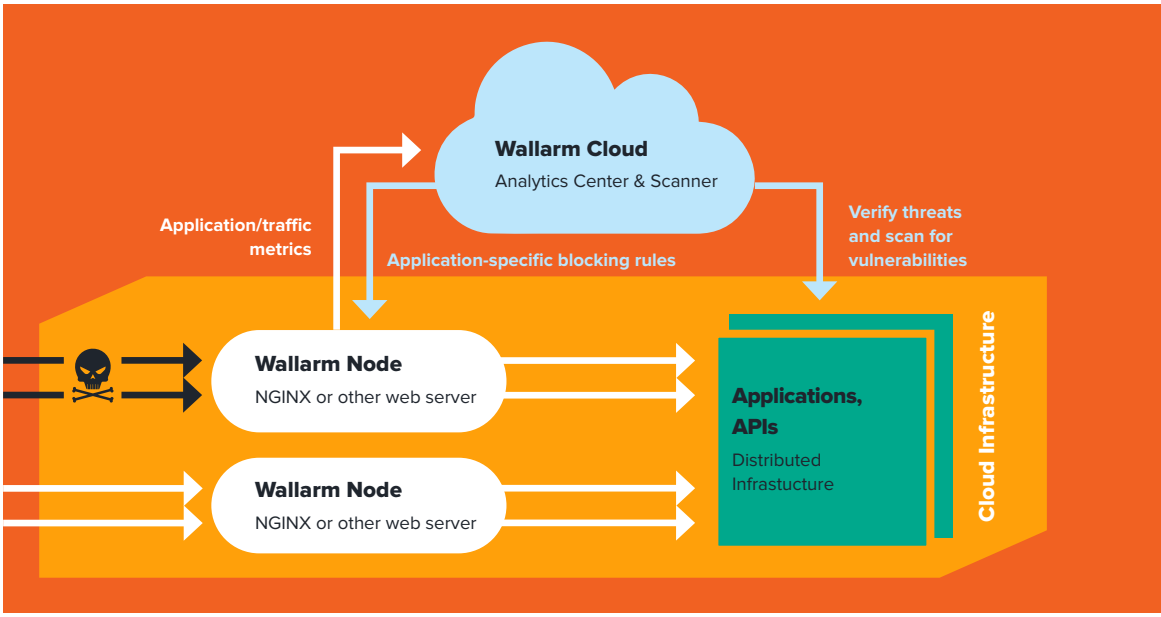
wallarm

wallarm.com

Adaptive application security

Used by over a hundred of SaaS and enterprise customers, the platform delivers attack mitigation and scanning functionality. Attack mitigation includes NG WAF and bot protection while security scanner discovers the network perimeter, probes for application-specific vulnerabilities and performs active threat verification.

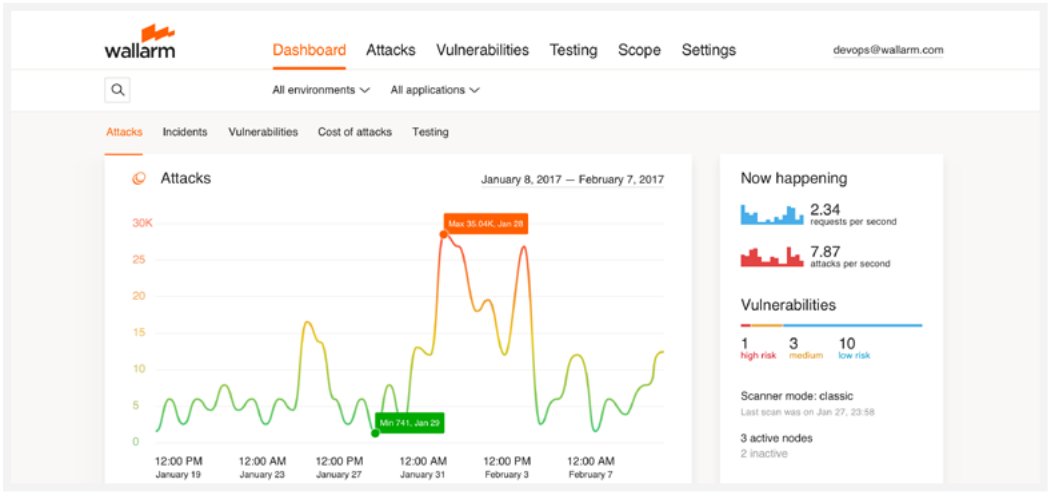
Application protection and security testing rely on the common AI-powered platform, which learns from stateless traffic to create application-specific dynamic rules. To further improve the accuracy and refine security policies, AI also learns from the feedback loop between the protection and scanning modules.



Wallarm hybrid architecture makes it well suited for SaaS applications. The solution scales horizontally. Filtering nodes can be installed with load balancing nodes, such as NGINX Plus, to achieve scale with little overhead.

Initial statistical analysis of the traffic is performed locally by the nodes. Then anonymized app traffic statistics is sent to Wallarm Cloud for AI analysis to develop app specific blocking security rules which are downloaded to the nodes.

> **With active threat detection, we are no longer overswamped with tons of useless events. As all the payloads from malicious requests are analyzed with a cloud scanner, we don't need to do this manually. Adaptive security rules allowed us to use WAF in blocking mode which was almost impossible previously.**
>
> **Mike Chadwick,**
> **VP of Engineering of Acronis**



SIGN UP FOR A FREE TRIAL!

request@wallarm.com **(415) 940-7077**